JOURNAL OF ALGEBRA **184,** 1041–1051 (1996)
ARTICLE NO. 0297

Solutions to Central Embedding Problems Are Constructible*

John R. Swallow†

Department of Mathematics, Davidson College, Davidson, North Carolina 28036

Let p be a prime and K a field of characteristic not p containing the pth roots of unity. Suppose that $1 \to \mathbb{Z}/p\mathbb{Z} \to H \to G \to 1$ is a central embedding problem of Galois groups, where $G = \mathrm{Gal}(L/K)$. We show that an isomorphism from a matrix ring to any algebra representative of the cohomological obstruction of the embedding problem determines explicitly solutions to the embedding problem.

1. INTRODUCTION

Obstructions of the solvability of central embedding problems associated to orthogonal representations have been studied by Serre [Se1], Fröhlich [Fr], and Crespo [Cr1, Cr2]; taken together, their results show that (1) for many central $\mathbb{Z}/2\mathbb{Z}$-embedding problems the obstruction can be written as a product of Hasse–Witt invariants and that (2) if the product is trivial, explicit solutions to the embedding problem may be found. For central $\mathbb{Z}/p\mathbb{Z}$-embedding problems, Fröhlich [Fr, Appendix] and Crespo [Cr3] proved similar results for central embedding problems associated to projective representations, but the hypotheses on the representations are very restrictive. In [Sw3] the author generalized these results to allow for twisted orthogonal and projective representations, permitting the application of their methods to a wider class of embedding problems. For a survey of these and other results, see [GSS]. In this paper we generalize these

* This work was derived from the author's thesis, written under the thoughtful supervision of Walter Feit. Research supported in part by NSF grant DMS-91-08148.
† E-mail: joswallow@davidson.edu.

0021-8693/96 $18.00

results to provide, for any central $\mathbb{Z}/p\mathbb{Z}$-embedding problem over a field of characteristic not p containing the pth roots of unity, a method for constructing solutions when the obstruction can be shown to be trivial via an explicit isomorphism of a matrix ring to an algebra representative of the obstruction.

In all that follows let K be a field of characteristic not p containing the pth roots of unity μ_p, K^s be the separable closure of K, Ω_K be the absolute Galois group of K, and L/K be a finite Galois extension with group G. The central embedding problem

$$1 \to \mathbb{Z}/p\mathbb{Z} \to H \to G \to 1$$

is solvable if and only if the obstruction to the embedding problem, defined as the inflation from G to Ω_K of the class of the 2-cocycle a in $H^2(G, \mathbb{Z}/p\mathbb{Z})$ corresponding to the group extension, is trivial [Ho]. Note that since $\mu_p \subset K$, the obstruction can therefore be represented by an element of the p-torsion of the Brauer group of K, by virtue of the isomorphism $H^2(\Omega_K, \mu_p) \cong \mathrm{Br}_p(K)$. If the obstruction is trivial, the solutions to the embedding problem are the fields $L((r\gamma)^{1/p})$ with r running over K^*/K^{*p} and γ an element in L^* satisfying $\gamma^g = b_\gamma^p \gamma$ for $g \in G$ with b_γ in L^* such that $b_g^{g'} b_{g'} b_{gg'}^{-1} = a_{g,g'}$ for $g, g' \in G$.

Let $\delta\colon H^1(\Omega_K, PGL(A \otimes K^s)) \to H^2(\Omega_K, K^{s*})$ be the cohomological coboundary homomorphism associated to the exact sequence

$$1 \to K^{s*} \to GL(A \otimes K^s) \to PGL(A \otimes K^s) \to 1$$

for A a central simple K-algebra. We denote by $GL(A)$ ($PGL(A)$) the group (the projective group) of invertible elements of A. Now suppose that we have a subset $R(A \otimes K^s)$ of $GL(A \otimes K^s)$ such that, when restricted to R, the exact sequence becomes an exact sequence of sets (with distinguished identity element)

$$1 \to \mu_p \to R(A \otimes K^s) \to PR(A \otimes K^s) \to 1.$$

Denote by δ_R the corresponding coboundary

$$\delta_R\colon H^1(\Omega_K, PR(A \otimes K^s)) \to H^2(\Omega_K, \mu_p).$$

We propose to represent the 2-cocycle a as $\delta_R(\inf_G^{\Omega_K} \alpha)$ for certain $\alpha \in H^1(G, PR(A \otimes L))$ and R. The properties of R and α that we will need we encapsulate in the following definition:

DEFINITION. Let $1 \to \mathbb{Z}/p\mathbb{Z} \to H \to G \to 1$ be a central embedding problem and

$$\rho\colon H \to GL(A)$$

be an injective homomorphism. Equip A, as a K-vector space of dimension m^2, with an H-action by virtue of multiplication by the image of H under ρ. Let $\{X_{ij}\}_{i,j=1}^{m}$ be a fixed K-vector space basis of A and let $N = K[\{X_{ij}\}]^H$ be the algebra of H-invariant K-polynomials on this basis.

An *invariant family* with respect to the embedding problem and the data (A, ρ) is a set $S = \{P_1, P_2, \dots, P_v\}$ of homogeneous degree p polynomials from N with the property that $(\mathrm{Det}_m^t \circ \chi)$ lies in the ideal

$$(P_1, P_2, \dots, P_v) \subset K^s\left[\{X_{ij}\}\right]$$

for some $t \in \mathbb{N}$ and some isomorphism $\chi\colon A \otimes K^s \to \mathrm{Mat}_m(K^s)$.

Let $\mathbf{P} := (P_1, P_2, \dots, P_v)\colon A \otimes K^s \to (K^s)^v$ be the cartesian product of the polynomial functions P_i. If S is an invariant family we say that $R = \mathbf{P}^{-1}(\mathbf{P}(1))$ is the *invariant space* associated to the invariant family.

Note that $\mathrm{Det} \circ \chi$ is the reduced norm of A for any choice of χ. Also, note that we must have that $\mu_p(K) \in A$ is the intersection of K^s with the inverse image of $\mathbf{P}(1)$ under the map $\mathbf{P}$, since $\mathbf{P}(1) \neq \mathbf{0}$ and $\mathbf{P}(xa) = x^p\mathbf{P}(a)$ for $x \in K^s$ and $a \in A \otimes K^s$.

From such a representation of the 2-cocycle a, together with an isomorphism from a matrix ring to the Galois twist of A, we shall derive a required element γ from a suitable element in $A \otimes L$. We shall further show that any 2-cocycle a can be so represented.

2. MAIN THEOREMS

THEOREM A. *Let* $1 \to \mathbb{Z}/p\mathbb{Z} \to H \to G \to 1$ *be a central extension of finite groups with* $G = \mathrm{Gal}(L/K)$, *A be a central simple algebra over K, and* $\rho\colon H \to GL(A)$ *be an injective homomorphism such that there exists an invariant family* $S = \{P_1, P_2, \dots, P_v\}$ *and the kernel of the group extension is mapped onto* μ_p.

The obstruction to the embedding problem is then given by the product $[B][A]^{-1}$ *in the Brauer group of K, where* $[B]$ *is the algebra given by Galois cohomology associated to the algebra A and* $\overline{\rho'}$, *where* $\rho'\colon G \to PGL(A)$ *is the projective representation given by factoring* ρ *by the center of A and where* $\overline{\rho'}$ *is the class of the* 1*-cocycle* ρ' *in the cohomology group* $H^1(G, PGL(A \otimes L))$.

The embedding problem is solvable if and only if there exists a K-isomorphism $h\colon B \to A$, *and if such an isomorphism exists, then there exists an element* $z \in A \otimes L$, *which may be explicitly constructed, such that not all* $P_i(z) = 0$ *and such that for any nonzero* $P_i(z)$ *the complete set of solutions to the embedding problem is* $\{L((r\gamma)^{1/p})\colon r \in K^*\}$ *with* $\gamma = P_i(z)$.

Proof. The 1-cocycle $\overline{\rho'}$ corresponds under Galois cohomology ([Se2, Chap. X]) to an L-equivalent central simple K-algebra $B = A_{\overline{\rho'}}$ with

$\dim_K B = \dim_K A$. The Brauer quotient $[B][A]^{-1}$ can be computed via the coboundary

$$\delta\colon H^1(\Omega_K, PGL(A \otimes K^s)) \to H^2(\Omega_K, K^{s*})$$

associated to the exact sequence

$$1 \to K^{s*} \to GL(A \otimes K^s) \to PGL(A \otimes K^s) \to 1$$

by finding the image of $\overline{\rho'}$. Because the central extension lies within the extension

$$1 \to \mu_p \to R(A \otimes K^s) \to PR(A \otimes K^s) \to 1,$$

we may choose a section of ρ' inside the invariant space $R(A \otimes K^s)$ so that the image of our 1-cocycle under the coboundary yields a 2-cocycle ρ^* in $Z^2(G, \mu_p)$ which must necessarily match that of the central extension. The obstruction is then the inflation of $\overline{\rho^*} \in H^2(G, \mu_p)$ into the p-torsion in the Brauer group $H^2(\Omega_K, \mu_p)$, which gives the quotient $[B][A]^{-1}$. Therefore the embedding problem is solvable if and only if A is K-similar to B. Note that by construction of B there is an L-isomorphism f from $B \otimes L$ to $A \otimes L$ such that $f^g f^{-1} = \rho'(g)$ for $g \in G$.

If the embedding problem is solvable, we then have a K-isomorphism h from B to A. The images of B under f and h being isomorphic, by Noether–Skolem there exists an element $z \in A \otimes L$ such that $z^{-1} f(\cdot) z = h(\cdot)$. Since the central extension of finite groups lies in the exact sequence and $\rho(H) \subset GL(A)$, there exist elements $x_g \in GL(A)$, $g \in G$, such that $x_{g'} x_g^{g'} x_{gg'}^{-1} = \rho^*(g, g')$ and conjugation by x_g in $GL(A)$ is identical to the action of $\rho'(g)$. Let $b_g = x_g z^g z^{-1}$, $g \in G$. One checks, as in [Cr1], that the b_g are in L and satisfy $b_g^{g'} b_{g'} b_{gg'}^{-1} = \rho^*(g, g')$ for $g, g' \in G$. Now since the P_i are homogeneous of degree p and P_i is invariant under multiplication by any element of $\rho(H)$, including the x_g, the relation $b_g z = x_g z^g$ gives us that

$$P_i(z)^g = b_g^p P_i(z).$$

Therefore any nonzero $P_i(z)$ is a γ such that all solutions to the embedding problem are given by $\{L((r\gamma)^{1/p})\colon\ r \in K^*\}$. Since $\mathrm{Det}^t \circ \chi \in (P_1, P_2, \ldots, P_v)$ for some $t \in \mathbb{N}$, not all the $P_i(z)$ can be zero, lest z be singular.

The determination of γ is constructive: the only components used in the calculation not explicitly constructed in the proof are the L-isomorphism f, which is derived from the construction of the twisted algebra B and can be determined, for instance, by a Poincaré series (see [Se2], Chap. X), and

z, which can be determined by solving a system of linear equations over K, as follows. Choose a vector space basis $\{e_i\}$ for A and define $f_{ij} \in L$ and $h_{ij} \in K$ by $f(e_i) = \sum f_{ij} e_j$ and $h(e_i) = \sum h_{ij} e_j$. Write $z = \sum z_{ij} e_i$ and equate corresponding coefficients of the e_i on each side of the defining relations for z, $f(e_i)z = zh(e_i)$. These equations will be linear in the z_{ij} over L. Choose a vector space basis for L over K and collect coefficients of this basis in the equations already derived; equating these coefficients yields a system of linear equations over K. Any solution to these equations yields an expression of z as a linear combination of the e_i; one must only check that the solution found is invertible. ∎

THEOREM B. *Let* $1 \to \mathbb{Z}/p\mathbb{Z} \to H \to G \to 1$ *be a central extension of finite groups with* $G = \mathrm{Gal}(L/K)$. *Then for each* $m \in \mathbb{N}$ *there exist a central simple K-algebra A of dimension* $(m|G|)^2$ *and an injective homomorphism* ρ: $H \to GL(A)$ *such that an invariant family S exists and* ρ *sends the kernel of the embedding problem to* μ_p.

Proof. Induce up to the full group H a one-dimensional faithful linear representation of the kernel $\mathbb{Z}/p\mathbb{Z}$. The elements mapping to the center are then precisely those in the kernel $\mathbb{Z}/p\mathbb{Z}$. Then consider the direct product of m copies of this representation. This provides a projective, untwisted representation ρ of G in $PGL_{m|G|}(K)$ whose lift in $GL_{m|G|}$ contains H. Let A then be $\mathrm{Mat}_{m|G|}(K)$. Now choose S to be the set of those degree p polynomials which are the inner products of the $(p-1)$st powers of elements of one column with the original elements in another column. As our induced representation has exactly one nonzero element in each row and column, and this element is a pth root of unity, each polynomial in S will be an invariant and the values of the polynomials for $w \in S$ will all be 1 or 0. Also, if all these invariants are zero, the rank of the matrix must be less than $m|G|$, hence singular. By Hilbert's Nullstellensatz, some multiple of the determinant is in the ideal in $K^s[\{X_{ij}\}_{i,j}]$ generated by S. Finally, since the only scalars which will yield 1 or 0 under all of these invariants are the pth roots of unity, our conditions are satisfied. ∎

COROLLARY. *Any central embedding problem can be constructively solved, given an explicit isomorphism from a matrix ring to an algebra representative of the cohomological obstruction.*

Remark. When the ground field does not contain the pth roots of unity (and even when the extension is not central), it is possible to recast the embedding problem as a central one over a field containing the pth roots of unity; see [Ho] and [Le]. In [Le] it is shown that solutions to the recast embedding problems provide solutions to the original problems. These

methods require the determination of the Galois group and actions of the pull-back of G and $G_p = \mathrm{Gal}(K(\mu_p)/K)$.

3. EXAMPLES

Example 1: *The Serre–Fröhlich–Crespo orthogonal case*. The explicit construction theorems of [Cr1] and [Cr2] for the orthogonal representations appearing in [Se1] and [Fr] correspond to Theorem A, as follows. The algebra A is the Clifford algebra C of the quadratic form, if the rank of the form is even, and is the even part C^+ of the Clifford algebra, if the rank of the form is odd. The invariant family is then the set S of polynomials on the matrix coefficients of the Clifford algebra (given an appropriate matrix representation) given by the relationship $i(m) \cdot m = I$, $m \in C$, where $i: C \to C$ is the unique involute antiautomorphism of the Clifford algebra and I is the identity element of C. The associated group R then contains the group $\widetilde{Pin}(q)$ (see [Fr]) and PR contains $O(q)$.

Example 2: *The Fröhlich–Crespo projective Case*. The explicit construction theorem in [Cr3] for the projective representations appearing in [Fr, Appendix] corresponds to the case in which the algebra A has degree p, the invariant family is the set S containing the one element given by the reduced norm, and the associated group R is $SL(A)$.

Example 3: $\mathbb{Z}/p^2\mathbb{Z}$ *extensions of* $\mathbb{Q}(\mu_p)$. While $\mathbb{Z}/p^2\mathbb{Z}$ fields over $\mathbb{Q}(\mu_p)$ have been previously constructed in [Ma] and [Sw3], explicit construction methods that employ (untwisted) orthogonal or projective representation have not handled this case. In particular, the method of [Cr3] calls for a faithful degree p representation of $\mathbb{Z}/p^2\mathbb{Z}$ over $\mathbb{Q}(\mu_p)$ with the image of reduced norm 1, but such representations do not exist. We use a projective representation and Theorem A to recover the explicit construction.

Let K be a field of characteristic not p containing the pth roots of unity, such as $\mathbb{Q}(\mu_p)$. Any $\mathbb{Z}/p\mathbb{Z}$ extension is given by $L = K(d^{1/p})$ for d in $K^* \setminus K^{*p}$. Let σ be a generator of the Galois group $\mathbb{Z}/p\mathbb{Z}$, such that $(d^{1/p})^{\sigma-1} = \xi_p$, where ξ_p is a primitive pth root of unity.

Denote by $(s_1, s_2)_p$ the central simple algebra over K of degree p given by generators i, j with $i^p = s_1$, $j^p = s_2$, and $ji = \xi_p ij$ for $s_1, s_2 \in K^*$. Let $A = (1, \xi)_p$ be the central simple algebra of Theorem A and define the required projective representation by taking the one in which σ is sent to conjugation by j. The lift of the image in $PGL(A)$ to A is then a cyclic group of order p^2. Consider the following matrix representation in $\mathrm{Mat}_p(K)$ of A: $i \mapsto \mathrm{diag}(1, \xi, \xi^2, \ldots, \xi^{p-1})$, $j \mapsto (m_{vw})$, where $m_{vw} = 1$ if $w - v \equiv 1 \bmod p$ and $v \neq p$; $m_{p1} = \xi$; and $m_{vw} = 0$ otherwise. One invariant

family is then that of Theorem B: the collection of dot products of $p-1$st powers of each column with each column.

The obstruction, as given by Galois cohomology, is the algebra $(d,\xi)_p$, with the L-isomorphism given by $f\colon (d,\xi)_p \to (1,\xi)_p$ with $f(i)=d^{1/p}i$, $f(j)=j$. If the primitive p^2th roots of unity are in K, the obstruction is trivial and we know that the set of solution fields is

$$\left\{K\left((rd^{1/p})^{1/p}\right)\colon r\in K^*\right\}.$$

Otherwise, this obstruction is equivalent to the existence of an element $y\in K(\xi^{1/p})^*$ such that $N_{K(\xi^{1/p})/K}y=d$. Suppose such a y exists and write it as $\sum_{\nu=0}^{p-1}k_\nu\xi^{\nu/p}$. From [Cr3] we know that a z of Theorem A is given by any nonzero

$$\sum_{\nu_1,\,\nu_2\in\{0,1,\ldots,p-1\}} f(i)^{\nu_1}f(j)^{\nu_2}g_{mn}(j)^{-\nu_2}g_{mn}(i)^{-\nu_1},$$

where g is a K-isomorphism from $(d,\xi)_p$ to $(1,\xi)_p$ and we define the K-isomorphisms g_{mn} from $(d,\xi)_p$ to $(1,\xi)_p$ by $g_{mn}(i)=\xi^m g(i)$, $g_{mn}(j)=\xi^n g(j)$, for $m,n\in\{0,1,\ldots,p-1\}$. Then $f(a)z=zg_{mn}(a)$ for $a\in A$.

A K-isomorphism $g\colon (d,\xi)_p\to(1,\xi)_p$ is defined by $g(i)=i\cdot\sum_{\nu=0}^{p-1}k_\nu j^\nu$, $g(j)=j$. Then the z of Theorem A can be computed as

$$p\cdot\sum_{\nu_1\in\{0,1,\ldots,p-1\}} f(i)^{\nu_1}g_{m0}(i)^{-\nu_1}$$

since $f(j)=g(j)$; from [Cr3] we know that for some $m\in\{0,1,\ldots,p-1\}$, such a z will be nonzero. Using the matrix representation for A above, together with Theorem A, we then have the following result:

PROPOSITION. *Let K be a field of characteristic not p containing the pth roots of unity.*

(a) *If K contains a primitive p^2th root of unity, then a $\mathbb{Z}/p\mathbb{Z}$ field $L=K(d^{1/p})$ can always be embedded in a $\mathbb{Z}/p^2\mathbb{Z}$ field; the complete set of such fields is*

$$\left\{K\left((rd^{1/p})^{1/p}\right)\colon r\in K^*\right\}.$$

(b) *If K does not contain a primitive p^2th root of unity, then a $\mathbb{Z}/p\mathbb{Z}$ field $L=K(d^{1/p})$ can be embedded in a $\mathbb{Z}/p^2\mathbb{Z}$ field if and only if there exists an element $y\in K(\xi^{1/p})^*$ such that $N_{K(\xi^{1/p})/K}y=d$. If one exists, write $y=\sum_{\nu=0}^{p-1}k_\nu\xi^{\nu/p}$. Define matrix $M=(m_{vw})$ by $m_{vw}=\xi^v k_{w-v}$ if $w-v\geq 0$*

and $m_{vw} = \xi^{v+1}k_{w-v+p}$ *if* $w - v < 0$. *Define matrix* $F = \operatorname{diag}(d^{1/p}, \xi d^{1/p}, \xi^2 d^{1/p}, \ldots, \xi^{p-1}d^{1/p})$. *Let*

$$z_b = p\sum_{\nu=0}^{p-1}\left(\frac{\xi^b}{d}I\right)F^\nu M^{p-\nu}.$$

The complete set of $\mathbb{Z}/p^2\mathbb{Z}$ *fields into which* L/K *can be embedded is*

$$\left\{K\left((r\gamma)^{1/p}\right): r \in K^*\right\}$$

for γ *any nonzero dot product of the* $p-1$*st power of one column with another column of* z_b, *for any* $b \in \{0, 1, \ldots, p-1\}$, *and there must be some nonzero such dot product for some* b.

Example 4: *DC-extensions of fields of characteristic not* 2. Let DC be the group

$$\langle x, y, z | x^2 = y^2 = z^4 = 1,\ y^{-1}xy = xz^2,\ [x, z] = [y, z] = 1\rangle,$$

which is a central product of a dihedral group of order 8 with a cyclic group of order 4. This group has been studied in the context of the embedding problem

$$1 \to \mathbb{Z}/2\mathbb{Z} \to DC \to (\mathbb{Z}/2\mathbb{Z})^3 \to 1$$

in various papers, where the obstruction to the embedding problem as well as explicit constructions of DC extensions from the $(\mathbb{Z}/2\mathbb{Z})^3$ extension have been determined. In [Cr2] the method of Example 1 is used, but since the quadratic form isometry used is not equivalent to the triviality of the obstruction, the method does not characterize all DC extensions. (See [Cr2, Theorem 5] and [GSS, Theorem 4.3.2].) A complete characterization of all DC extensions is given in [MiSm], using normic relationships instead of isometries. We use our method to find a complete characterization of DC extensions using quadratic form isometries, in the spirit of [Wi]. This method was used to achieve the statement characterizing all DC extensions in [GSS, Theorem 4.3.4].

Let K be a field of characteristic not 2, a_1, a_2, and a_3 be linearly independent nonsquares in K^*, L be the field $K(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$, and σ_i, $1 \le i \le 3$, be the generators of $\operatorname{Gal}(L/K)$ given by $(\sqrt{a_i})^{\sigma_j - 1} = (-1)^{\delta_{ij}}$. Let DC be presented as above and consider the embedding problem $DC \to (\mathbb{Z}/2\mathbb{Z})^3$ given by the homomorphism $x \mapsto \sigma_1$, $y \mapsto \sigma_2$, $z \mapsto \sigma_3$. The obstruction to the embedding problem is the product of quaternion algebras $(a_1, a_2)(a_3, -1) \in \operatorname{Br}_2(K)$; this is computed, for instance, in [MiSm].

The obstruction is trivial if and only if the quadratic forms

$$Q_1 := \langle a_1a_3, a_2a_3, a_3\rangle$$

and

$$Q_2 := \langle 1, 1, a_1a_2a_3\rangle$$

are K-equivalent, since Q_1 and Q_2 are of rank 3 and have discriminants in the same square class. Let $P = (p_{ij})_{1 \le i, j \le 3}$ be a matrix such that $P^t[Q_2]P = [Q_1]$. Without loss of generality we may assume that $\det P = a_3$.

Let A be the central simple algebra given by the tensor product of two quaternion algebras $(1, 1)$ and $(1, 1)$, with generators i, j, k, l such that $i^2 = j^2 = k^2 = l^2 = 1$, $ji = -ij$, $lk = -kl$, $ik = ki$, $il = li$, $jk = kj$, and $jl = lj$. Let ρ be the homomorphism from DC to $GL(A)$ given by $x \to i$, $y \mapsto j$, $z \mapsto kl$; note that ρ maps the kernel of the embedding problem into ± 1. For an invariant family we use the set of dot products of columns in the following representation of A in $\mathrm{Mat}_4(K)$:

$$i \mapsto M_i = \big((M_i)_{wv}\big), \qquad j \mapsto M_j = \big((M_j)_{wv}\big),$$
$$k \mapsto M_k = \big((M_k)_{wv}\big), \qquad l \mapsto M_l = \big((M_l)_{wv}\big),$$

where $(M_i)_{11} = (M_i)_{33} = 1$, $(M_i)_{22} = (M_i)_{44} = -1$, $(M_i)_{wv} = 0$ otherwise; $(M_j)_{12} = (M_j)_{21} = (M_j)_{34} = (M_j)_{43} = 1$, $(M_j)_{wv} = 0$ otherwise; $(M_k)_{11} = (M_k)_{22} = 1$, $(M_k)_{33} = (M_k)_{44} = -1$, $(M_k)_{wv} = 0$ otherwise; $(M_l)_{13} = (M_l)_{24} = (M_l)_{31} = (M_l)_{42} = 1$, $(M_l)_{wv} = 0$ otherwise.

The twisted algebra B corresponding to A and ρ is the tensor product of two quaternion algebras $(a_2, a_1)(a_3, a_3)$; the L-isomorphism of A to B inside $A \otimes L$ is given by $f(i) = \sqrt{a_2}\,i$, $f(j) = \sqrt{a_1}\,j$, $f(k) = \sqrt{a_3}\,k$, and $f(l) = \sqrt{a_3}\,l$. Our matrix P gives us a K-isomorphism g from A to B as follows. Let $u_1 = i$, $u_2 = j$, $u_3 = ij((l + kl)/2 + (-a_1a_2a_3)(l - kl)/2)$, $u_4 = ijk$; $w_1 = p_{11}u_1 + p_{21}u_2 + p_{31}u_3$, $w_2 = p_{12}u_1 + p_{22}u_2 + p_{32}u_3$, $w_3 = p_{13}u_1 + p_{23}u_2 + p_{33}u_3$, $w_4 = u_4$. Then our K-isomorphism is given by $g(i) = w_2w_3w_4/a_3$, $g(j) = w_1w_3w_4/a_3$, $g(k) = w_3$, and $g(l) = w_3w_4$.

The element z can be found by taking the sum

$$\sum_{\nu_1, \nu_2, \nu_3, \nu_4 \in \{0, 1\}} f(i)^{\nu_1} f(j)^{\nu_2} f(k)^{\nu_3} f(l)^{\nu_4} g(l)^{-\nu_4} g(k)^{-\nu_3} g(j)^{-\nu_2} g(i)^{-\nu_1}$$

[Cr2]. We form z in our representation of $A \otimes L$ in $\mathrm{Mat}_4(L)$, and, in order to evaluate the members of the invariant family on z, we consider the dot products of the columns. We find that dot products of distinct columns always yield 0. Instead, we take the dot product of the first

column with itself, and the resulting γ is then

$$\begin{aligned}
&\frac{2\left(\sqrt{a_1a_2a_3}-1\right)^2}{a_1a_2a_3}\\
&\quad\times\Big(a_1a_2a_3-2a_2\sqrt{a_1a_3}\,p_{11}+2a_1\sqrt{a_2a_3}\,p_{22}\\
&\qquad+a_2p_{11}^2+a_1p_{12}^2+a_1a_2p_{13}^2\\
&\qquad+a_2p_{21}^2+a_1p_{22}^2+a_1a_2p_{23}^2+a_1a_2^2a_3p_{31}^2\\
&\qquad+a_1^2a_2a_3p_{32}^2+a_1^2a_2^2a_3p_{33}^2\\
&\qquad+2\sqrt{a_1a_2}\,p_{12}p_{21}-2\sqrt{a_1a_2}\,p_{11}p_{22}-2a_1a_2a_3\sqrt{a_1a_2}\,p_{33}\\
&\qquad+2a_1a_2\sqrt{a_2a_3}\,p_{11}p_{33}-2a_1a_2\sqrt{a_2a_3}\,p_{31}p_{13}\\
&\qquad-2a_1a_2\sqrt{a_1a_3}\,p_{22}p_{33}+2a_1a_2\sqrt{a_1a_3}\,p_{23}p_{32}\Big).
\end{aligned}$$

Reducing the last factor with a Gröbner basis corresponding to the relationships on the p_{ij} given by $P^t[Q_2]P=[Q_1]$, we have that γ is

$$8\left(\sqrt{a_1a_2a_3}-1\right)^2\left(1-\frac{p_{11}}{\sqrt{a_1a_3}}+\frac{p_{22}}{\sqrt{a_2a_3}}-\sqrt{a_1a_2}\,p_{33}\right),$$

whence the complete set of DC extensions of L is given by

$$\left\{L\left(\sqrt{r\left(1-\frac{p_{11}}{\sqrt{a_1a_3}}+\frac{p_{22}}{\sqrt{a_2a_3}}-\sqrt{a_1a_2}\,p_{33}\right)}\right):r\in K^*\right\}.$$

We have thus proved the following result:

PROPOSITION. *The complete set of DC extensions of a field K of characteristic not 2 is given by fields*

$$K\left(\sqrt{a_1},\sqrt{a_2},\sqrt{a_3},\sqrt{r\left(1-\frac{p_{11}}{\sqrt{a_1a_3}}+\frac{p_{22}}{\sqrt{a_2a_3}}-\sqrt{a_1a_2}\,p_{33}\right)}\right),$$

where a_1, a_2, a_3 run through independent nonsquares in K^*; $P=(p_{ij})_{1\le i,j\le 3}$ runs through isometries $P^t[Q_2]P=[Q_1]$ with $\det P=a_3$, $[Q_1]=\operatorname{diag}(a_1a_3,a_2a_3,a_3)$, *and* $[Q_2]=\operatorname{diag}(1,1,a_1a_2a_3)$; *and r runs through K^*.*

ACKNOWLEDGMENTS

This work is derived from a portion of the author's doctoral thesis, written under the thoughtful supervision of Walter Feit. The author would also like to thank Roger Howe for a discussion connected with this work.

REFERENCES

[Cr1] T. Crespo, Explicit construction of $\tilde{A}_n$ type fields, *J. Algebra* **127** (1989), 452–461; erratum, *J. Algebra* **157** (1993), 283.

[Cr2] T. Crespo, Explicit solutions to embedding problems associated to orthogonal Galois representations, *J. Reine Angew. Math.* **409** (1990), 180–189.

[Cr3] T. Crespo, Embedding Galois problems and reduced norms, *Proc. Amer. Math. Soc.* **112** (1991), 637–639.

[Fr] A. Fröhlich, Orthogonal representations of Galois groups, Stiefel–Whitney classes and Hasse–Witt invariants, *J. Reine Angew. Math.* **360** (1985), 84–123.

[GSS] H. Grundman, T. Smith, and J. Swallow, Groups of order 16 as Galois groups, *Exposition. Math.* **13** (1995), 289–319.

[Ho] K. Hoeschmann, Zum Einbettungsproblem, *J. Reine Angew. Math.* **229** (1968), 81–106.

[Hu] B. Huppert, Endliche Gruppen I, *Grundlehren Math. Wiss.* **134** (1967).

[Le] A. Ledet, Subgroups of HolQ_8 as Galois groups, *J. Algebra* **181** (1996), 478–506.

[Ma] R. Massy, Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p, *J. Algebra* **109** (1987), 508–535.

[MiSm] J. Mináč and T. L. Smith, A characterization of C-fields via Galois groups, *J. Algebra* **137** (1991), 1–11.

[Se1] J.-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comment. Math. Helv.* **59** (1984), 651–676.

[Se2] J.-P. Serre, "Local Fields," Springer-Verlag, Berlin/New York, 1979.

[Sw1] J. Swallow, Constructive solutions to central embedding problems, Ph.D. Dissertation, Yale University, May 1994.

[Sw2] J. Swallow, Embedding problems and the $C_{16} \to C_8$ obstruction, Recent developments in the inverse Galois problems, *Contemp. Math.* **186** (1995), 75–90.

[Sw3] J. Swallow, Central p-extensions of $(p, p, \ldots, p)$-type Galois groups, *J. Algebra*, to appear.

[Wi] E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. Reine Angew. Math.* **174** (1936), 237–245.